St Mary's Catholic First School

E-Safety Policy

Bishop Wilkinson
Catholic Education Trust
Through Christ, in Partnership

Part of the Bishop Wilkinson Catholic Education Trust
Company Registration Number 07890590

Review Period	**November 2024**
Next Review Date	**November 2025**
Reviewed by	**Mrs. S. Oakes**

St Mary's Catholic First School

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake-news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young

adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping children safe in education - GOV.UK (www.gov.uk), and its advice for schools on:

- Teaching online safety in schools - GOV.UK (www.gov.uk)
- Preventing bullying - GOV.UK (www.gov.uk)and Cyber bullying: advice for headteachers and school staff (publishing.service.gov.uk)
- Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)

It also refers to the DfE's guidance on preventing radicailisation: The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK (www.gov.uk).

It reflects existing legislation, including but not limited to the Education Act 1996 (legislation.gov.uk) (as amended), the Education and Inspections Act 2006 (legislation.gov.uk)and the Equality Act 2010 (legislation.gov.uk). In addition, it reflects the Education Act 2011 (legislation.gov.uk), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Local Governing Committee

The Governing Committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The Governing Committee will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety as provided by the designated safeguarding lead (DSL).
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing committee.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a [weekly basis].
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:

-What are the issues? – What are the issues? - UK Safer Internet Centre
-Hot topics – Help & advice | Childnet
-Parent resource sheet – Parents and Carers resource sheet | Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:
It is also taken from the Relationships and sex education (RSE) and health education - GOV.UK (www.gov.uk).

All schools have to teach:

- Relationships and sex education (RSE) and health education - GOV.UK (www.gov.uk) in primary schools.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact.

By the **end of first school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition:

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
-Cause harm, and/or
-Disrupt teaching, and/or
-Break any of the school rules
If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should: --
-Delete that material, or
-Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
-Report it to the police*
* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)

- UKCIS guidance on Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school; these are to be handed into the office for the duration of the school day and pupils are not permitted to use them during:

-Lessons
-At Break Times
-Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school IT technician and or the IT dept at Bishop Wilkinson Catholic Education Trust.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  o Abusive, harassing, and misogynistic messages
  o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  o Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. These incidents will be recorded on our CPOMS system.

This policy will be reviewed every year by the Head Teacher. At every review, the policy will be shared with the governing committee. The review (such as this one: OS Audit - Online Safety Audit from LGfL | LGFL) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy.

Appendix 1: KS1-Acceptable Use Policy

Academic Year 2024-25

LGfL SafeguardED

Acceptable Use Policy (AUP) for KS1 PUPILS

My name is _____

To stay SAFE online and on my devices:	✓
1. I only USE devices or apps, sites or games if I am allowed to	
2. I ASK for help if I'm stuck or not sure; I TELL a trusted adult if I'm upset, worried, scared or confused	
3. I look out for my FRIENDS and tell someone if they need help	
4. If I get a FUNNY FEELING in my tummy, I talk to an adult	
5. I KNOW that online people aren't always who they say they are and things I read are not always TRUE	
6. Anything I do online can be shared and might stay online FOREVER	
7. I don't keep SECRETS 🚫 unless they are a present or nice surprise	
8. I don't have to do DARES OR CHALLENGES ❌, even if someone tells me I must.	
9. I don't change CLOTHES or get undressed in front of a camera	
10. I always check before SHARING my personal information or other people's stories and photos	
11. I am KIND and polite to everyone	

My trusted adults are:

_____ **at school**

_____ **at home**

Appendix 2: KS2 Acceptable Use Policy

LGfL SafeguardED Acceptable Use Policy (AUP) for KS2 PUPILS

Academic Year 2024-25

These statements can keep me and others safe & happy at school and home:
Digital 5 a day | Children's Commissioner for England (childrenscommissioner.gov.uk)

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.		15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.	
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.		16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.	
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.		17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.	
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.		18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.	
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.		19. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.	
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it maybe hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.		20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.	
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!		21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.	
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults.		22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.	

LGfL SafeguardED

Acceptable Use/Behaviours Policy (AUP) for PARENTS

- We would like to take this opportunity to signpost parents to parentsafe.lgfl.net, a dedicated one-stop portal offering parents support and advice on safe settings, parental controls and monitoring, apps and games, talking to children about life online, screentime and key topics from bullying to accessing pornography, extremism and gangs, fake news and more.

- We also recommend the Digital Family Agreement with example statements to help families agree on shared expectations around time spent on devices, and ground rules like no phones at the table or in the bedroom at night-time.

Background

We ask all children, young people and adults involved in the life of St. Mary's Catholic First School to read and sign an Acceptable Use/Behaviours Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child will also be asked signed an AUP which is available in school.

We tell your children that **they should not behave any differently when they are out of school or using their own device or on a home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read St. Mary's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Mrs. S. Oakes (Headteacher) (01434) 603 791.

LGfL SafeguardED

Acceptable Use/Behaviours Policy (AUP) for PARENTS

What am I agreeing to?

1. I understand that St. Mary's uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring. More detail of this can be found in our online safety policy.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I will support my child to follow the school's policy regarding bringing devices to school. Children are not permitted to bring devices to school. In year 4, some pupils begin bringing mobile devices to school. These are locked in the main office for the duration of the school day and only given at the end of the school day.
7. I understand that my child might be contacted online on by class teachers and only about their learning, wellbeing or behaviour. If they are contacted by someone else or staff ask them to use a different app to chat, they will tell another teacher. If a particular member of staff, behaves inappropriately contact the Headteacher who is also the Designated Safeguarding Lead. See the Safeguarding & Child Protection Policy: Safeguarding-and-child-protection-policy-2023-2024-OW.pdf (hexhamstmarys.uk) or the Complaints Policy: BWCET-Complaints-Policy-2024-25.docx (live.com)
8. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
9. Parents are kindly asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
10. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
11. I will follow St. Mary's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
12. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...
13. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
14. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
15. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age-appropriate content. Find out more at parentsafe.lgfl.net
16. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
17. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
18. I can find out more about online safety at St. Mary's by reading the full Online Safety Policy here and can talk to class teachers, Designated Safeguarding Leads and/or the Headteacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____
~~~~~~~~~~~~~~~~~~

Appendix 3b: Acceptable Use Policy-Staff, Governors & Volunteers

LGfL SafeguardED

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS 2024-25

Background

We ask everyone involved in the life of St. Mary's to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, [redacted] connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff, governors and volunteers) have particular legal / professional [redacted] and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online E-Safety Policy.

If you have any questions about this AUP or our approach to online safety, please speak to Sarah Oakes (0345 603 7974.

What am I agreeing to?

1. **(This point is for staff, governors & volunteers):**
   I have read and understood St. Mary's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best practice in this area.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult) and make them aware of new trends and patterns that I identify.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media). I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be experienced in the playground, corridors, toilets and other communal areas outside the classroom. understand the wellness tax.
5. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!
6. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

LGfL SafeguardED

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS 2024-25

8. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
10. I will check with Sarah Oakes (Headteacher/DSL) if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured.
11. I will follow best practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods. Please refer to approaches at: [redacted]
12. I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness. I will flag any concerns about [redacted] to the DSL.
13. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
14. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
15. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
16. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
17. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are over-blocking, I shall notify the school to inform regular checks and annual review of these systems.
18. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
19. I will not contact or attempt to contact any pupil or to access their contact details (including their username/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.

LGfL SafeguardED

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS 2024-25

20. If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.
21. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online E-Safety policy. If I am ever not sure, I will ask first.
22. I will not use any new technology or download any apps without agreement from the Headteacher.
23. I will not use a mobile hotspot to provide internet to any device I use in school.
24. I agree to [redacted] whether or not I am on site or using a school device, platform or network.
25. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
26. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
27. I will only use genuine AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

LGfL SafeguardED

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS 2024-25

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by Headteacher

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems: _____

Additional permissions (e.g. admin) _____

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	